RSAC 2025 Conference

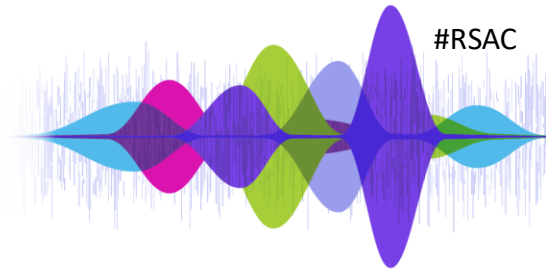
Many Voices.
One Community.

SESSION ID: LAB3-W08

Case Studies in Vulnerability Prioritization

Audra Streetman

Senior Threat Intelligence Analyst
Splunk
Linkedin.com/in/audrastreetman

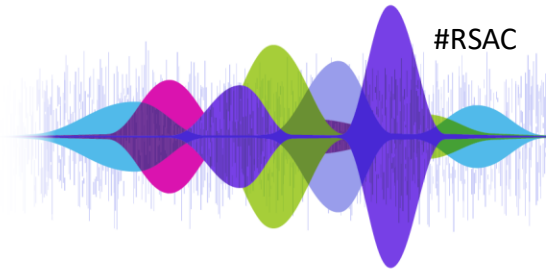


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



Agenda

- Introductions
- Evaluating a Vulnerability (5Ws)
- Group Discussion
- Case Studies: MOVEit Transfer, Log4j, HAFNIUM/Exchange
- Group Tabletop Exercise
- Vulnerability Databases and Scoring Methods

RSAC 2025 Conference

Introductions

Share your favorite/most disliked vulnerability and/or what you hope to gain from this Learning Lab.

Many Voices.
One Community.

RSAC 2025 Conference

Evaluating a Vulnerability

5Ws: Who, What, When, Where, Why

Many Voices.
One Community.

Evaluating a Vulnerability with the 5Ws

- **Who** is discussing vulnerabilities?
  - Peers
  - Industry Experts
  - Government Advisories

Online discourse may include fear-mongering and hyperbole.

Cisco Confidential

Evaluating a Vulnerability with the 5Ws

- **What** is the exploitability?
  - Is it remotely exploitable?
  - Is exploit code public?
  - What is the impact of successful exploitation?

Cisco Confidential

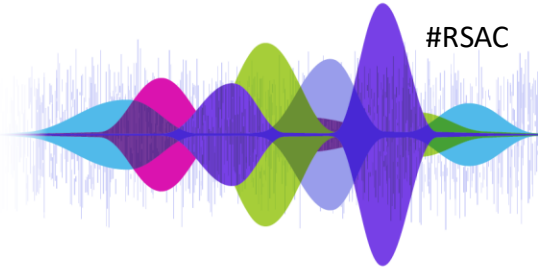
Evaluating a Vulnerability with the 5Ws

- **When** was it disclosed?
  - Was it a coordinated/responsible disclosure with a deadline to patch before public disclosure?
  - Is it actively exploited in the wild?
  - Was it exploited as a zero-day?

Evaluating a Vulnerability with the 5Ws

- **Where** does it exist in your environment?
  - Does it impact a software component listed in an SBOM or vendor advisory?
  - Is the impact of exploitation influenced by where the vulnerability is present in your environment?
  - Is it externally facing?
  - Is a patch available?

Evaluating a Vulnerability with the 5Ws



- Understanding the **Why**:
  - Does this vulnerability align with recent trends in adversary behavior?
  - Does it have a score, such as CVSS or EPSS?
    - These scores should not be the only factor in evaluating.
  - Is it listed in a database like the CISA KEV?

Cisco Confidential

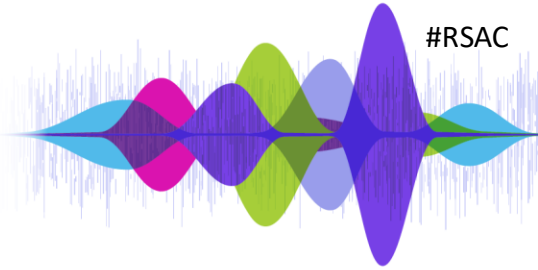
RSAC 2025 Conference

Group Discussion

What would you add to the 5Ws or highlight based on past experiences?

Many Voices.
One Community.

Case Study: MOVEit Transfer (2023)



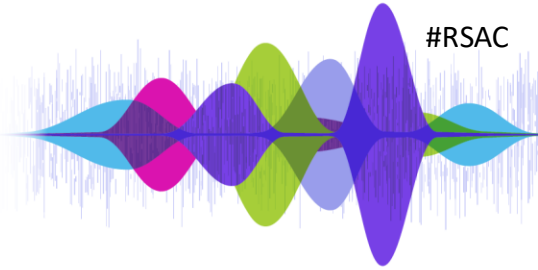
- Impact:
  - 95.7M Individuals and 2,773 organizations (source: Emsisoft)
- Lessons learned:
  - Adversary behavior can inform our expectations about the likelihood of exploitation
  - Simple attack chain + zero-day = higher priority
  - Supply chain considerations

Cisco Confidential

Case Study: Log4j (2021)

- Why this vulnerability was a high priority:
  - It was remotely exploitable.
  - It was publicly disclosed before a fix was available.
  - PoC exploit code circulated on the Internet.
  - Log4j is popular among Java developers and embedded into thousands of software packages and millions of systems worldwide.

Case Study: HAFNIUM/Exchange (2021)



- What happened:
  - Cyberespionage campaign targeting on-prem Exchange servers
  - Attributed to HAFNIUM, a China-nexus state sponsored threat group
- Lessons learned:
  - Consider the impact of downtime during the patching process
  - Patch gaps can lead to compromise (i.e., backdoors)

RSAC 2025 Conference

Tabletop Exercise

Tabletop Exercise 1

CloudSync

- RCE vulnerability in CloudSync 5.2, a cloud storage synchronization service that is widely deployed in corporate environments, with ~2,000 Internet-exposed instances.
- Allows execution of arbitrary commands on affected servers by sending a specially crafted API request.
- High exploitability, requires no authentication or user interaction.
- Public disclosure by a third-party researcher overnight.
- No patch yet, but mitigations exist (disable vulnerable API endpoint).

HR IDOR

- An Insecure Direct Object Reference (IDOR) vulnerability exists in an HR portal used by ~2,500 small-to-medium businesses (SMBs).
- An attacker can modify the employee_id parameter in API requests to access confidential personal details and tax documents.
- Exploitability is relatively easy with knowledge of API requests.
- Reported by a researcher for coordinated disclosure with the vendor yesterday. A patch is available.
- Active exploitation observed in the wild.

Tabletop Exercise 2

SecurePay API

- Third-party payment processing API used by your e-commerce platform.
- API authentication bypass vulnerability to initiate fraudulent transactions using specially crafted API requests.
- Remotely exploitable, no authentication or user interaction required.
- 1,500+ businesses use this payment API.
- Privately reported by a researcher, but PoC exploit code leaked on a forum.
- Vendor is rolling out a patch in 48 hours, no immediate fix available.
- Mitigation: rate-limiting and API request monitoring can reduce risk but not prevent exploitation.

CoreX Hypervisor

- Your organization's virtualization platform hosts thousands of production workloads.
- Memory corruption vulnerability in the hypervisor allows a guest VM to escape and execute code on the host, leading to full server takeover.
- Requires chaining vulnerabilities, PoC exists.
- Allows for privilege escalation and possible compromise of entire cloud environments.
- 500+ critical production servers affected.
- Researchers released detailed overview of the exploit methodology.
- Patch available, but applying it requires rebooting all hypervisors, leading to potential service downtime.

Tabletop Exercise 3

VaultDB Privilege Escalation

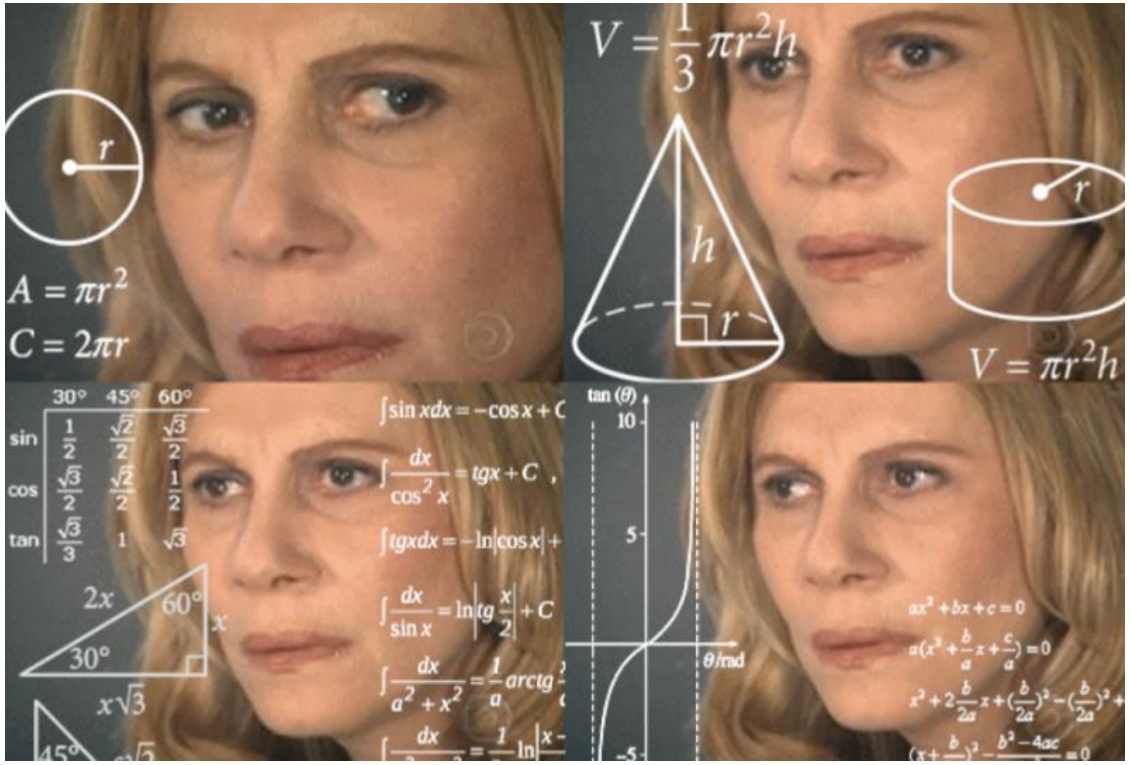
- Local privilege escalation via a misconfigured service that allows a low-privilege user to gain root access.
- Requires initial access but is trivial to execute once inside the network.
- Impact: full control over the database server.
- 500+ production database servers across multiple subsidiaries, none directly exposed to the Internet.
- Researcher reported the issue privately under coordinated disclosure.
- Patch available, but requires full database reboot, leading to downtime for critical operations.
- Workarounds exist but may introduce system instability.

WebPort SSRF Zero-Day

- Server-side request forgery (SSRF) allowing an attacker to manipulate API calls to gain unauthorized access to internal services.
- Can be exploited remotely without authentication but requires specific knowledge of the backend API structure.
- Impact: potential exposure of internal system metadata, limited access to internal services, possible lateral movement.
- 3,000+ internet-exposed instances.
- Public disclosure by third-party researcher.
- No patch available. Vendor estimates one week timeline.
- Mitigation: WAF rules can block most attack patterns, but bypasses are possible.

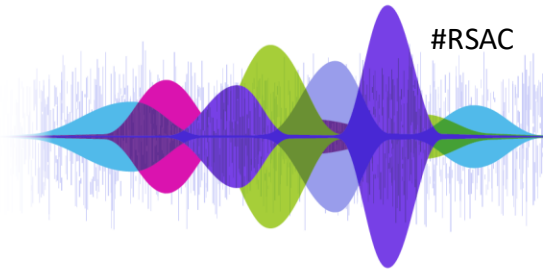
Databases and Scoring Methods

- CISA KEV
- NIST NVD
- CVE.ICU
- EPSS
- SSVC
- CSAF
- VEX
- Cisco VM
- OSV Schema
- OSS Index
- VulDB
- VISS
- The list goes on…



splunk> a CISCO company
RSAC 2025 Conference
Cisco Confidential

Apply What You Have Learned Today



- Next week you should:
  - Familiarize yourself with vulnerability databases and scoring methods.
- In the first three months following this presentation you should:
  - Study recent adversary behavior that could influence vulnerability exploitation (i.e., threat reports, advisories, cybersecurity news).
  - Evaluate patch management strategies to minimize downtime.
- Within six months you should:
  - Tailor your vulnerability management program to evaluate and prioritize vulnerabilities based on criticality and business context (the 5Ws).

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you!